

I. Authentication

- Two principals verify each others' identities
- Two flavors
 - **Direct authentication:** directly between two parties
 - **Indirect authentication:** uses a trusted third-party server
 - Called authentication server
 - E.g., A Verisign server